PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-238305**

(43)Date of publication of application : **31.08.1999**

(51)Int.Cl. **G11B 20/10**

(21)Application number : **10-040730**

(22)Date of filing : **23.02.1998**

(71) Applicant : **SONY CORP**

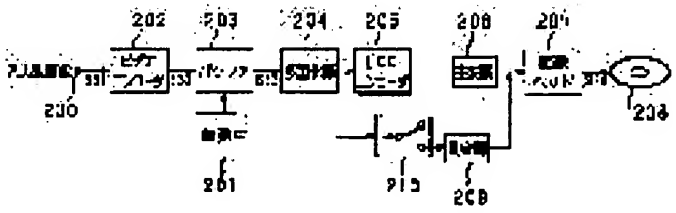
(72)Inventor : **SENDA YOSHINARI**
NAKAMURA MASANOBU

(54) DATA PROCESSING METHOD AND DATA RECORDING AND REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively prevent an illegal copy with an inexpensive and simple constitution by using plural modulation systems, generating a code word as to a specific sector with a modulation system different from that of other sectors and writing data for decoding the data of the other sectors normally in the specific sector.

SOLUTION: Encryption data of a key generating circuit 21 are supplied to an encoder buffer 203 together with video data from a video encoder 202 and they are multiplexed in time-division manner in a multiplexer 204 to be outputted. After the encryption data are added with an error correction code by an ECC encoder 205, the data are transmitted to a switch 210 to be written in the specific sector on an optical disk 208. The bit stream of the encryption data is modulated by a submodulation circuit 209 whose system is a modulation system entirely different from that of a main modulation circuit 206 by being changed over with a switch 210. Thus, the encryption data fail to function normally in a normal reproducing device and the reproducing of the data becomes impossible and the illegal copy is prevented.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－238305

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ

審査請求　未請求　請求項の数２　ＯＬ　（全５頁）

(21)出願番号　特願平10－40730

(22)出願日　平成10年(1998)２月23日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　千田　吉成
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　中村　政信
東京都品川区北品川６丁目７番35号　ソニー株式会社内

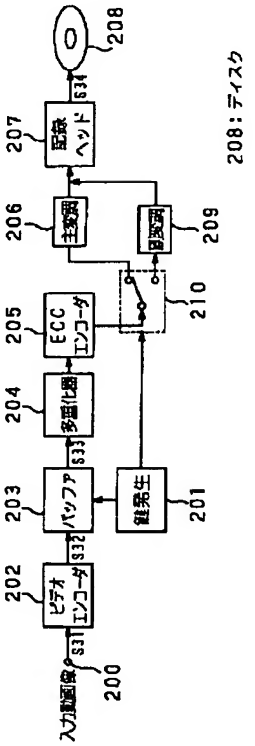
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　データ処理方法及びデータ記録再生装置

(57)【要約】

【課題】　暗号化鍵の管理が容易で且つ演算量も少なく、簡単なシステムでも実現でき、安価で簡単な構成であっても不法コピーを有効に防止し得る暗号化を可能とする。

【解決手段】　特定のセクタに対する他のセクタのデータを正常にデコードするための暗号化データを発生する鍵発生回路２０１と、暗号化データを特定のセクタに書き込むための多重化器２０４と、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成する副変調回路２０９と、特定のセクタに対する他のセクタについてコードワードを生成する主変調回路２０９と、それらの変調信号を光ディスク２０８に記録する記録ヘッド２０７とを有する。



【特許請求の範囲】
【請求項1】　少なくとも二つの変調方式を使用し、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成し、
上記特定のセクタには、他のセクタのデータを正常にデコードするためのデータを書き込むことを特徴とするデータ処理方法。
【請求項2】　少なくとも二つの変調方式を使用し、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成するコードワード生成手段と、
上記特定のセクタには、他のセクタのデータを正常にデコードするためのデータを書き込む書き込み手段と、
上記変調方式による変調信号を記録媒体に記録する記録手段と、
上記特定のセクタのデータを少なくとも二つの復調方式のうちの一の復調方式により復調する復調手段と、
上記特定のセクタの復調されたデータに基づき、上記他のセクタの復調データの正常再生を可能にする再生手段と、を有することを特徴とするデータ記録再生装置。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、例えばデータを暗号化してディスク等の記録媒体に記録する際に好適なデータ処理方法及びデータ記録再生装置に関する。
【0002】
【従来の技術】従来より、データの機密性を確保したり、あるいはデータに対する不正アクセスや、コピーの防止などのために、データを暗号化する事が一般的に行われている。
【0003】上記データの暗号化の手法としては、例えば、いわゆるＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などに代表される暗号方法が知られている。
【0004】
【発明が解決しようとする課題】しかし、この暗号方法は、鍵（暗号化鍵）の管理の難しさ、及びその演算量などから、小さな規模で実施するのが難しく、高度なシステムでの実施に限られていた。
【0005】また、近年は、不法コピーが問題となっており、特にディジタルデータの形態で頒布される著作物の著作権保護が必要になっている。特に、光磁気ディスクや光相変化ディスクなどの記録可能ディスクの大容量化が進むと、家庭レベルで多量の複製物が製造可能になり、これを防止することが課題となっている。
【0006】そこで、本発明は上述の実情に鑑みて提案されるものであり、暗号化鍵の管理が容易で且つ演算量も少なく、簡単なシステムでも実現でき、したがって、安価で簡単な構成であっても不法コピーを有効に防止し得る暗号化を可能とする、データ処理方法及びデータ記録再生装置を提案することを目的とする。
【0007】
【課題を解決するための手段】本発明のデータ処理方法は、少なくとも二つの変調方式を使用し、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成し、特定のセクタには他のセクタのデータを正常にデコードするためのデータを書き込むことにより、上述した課題を解決する。
【0008】また、本発明のデータ記録再生装置は、少なくとも二つの変調方式を使用し、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成する手段と、特定のセクタには他のセクタのデータを正常にデコードするためのデータを書き込む手段と、それらの変調信号を記録媒体に記録する手段と、特定のセクタのデータを少なくとも二つの復調方式のうちの一により復調する手段と、特定のセクタの復調されたデータに基づき、他のセクタの復調データの正常再生を可能にする手段とを有することにより、上述した課題を解決する。
【0009】
【発明の実施の形態】本発明に係るデータ処理方法及びデータ記録再生装置の一実施の形態について、図面を参照しながら説明する。
【0010】図1には、本発明に係るデータ処理方法及びデータ記録再生装置が適用される一実施の形態のシステムにおける記録系（エンコード系）の構成例を示す。この図1の構成では、ディジタル信号の一例として、複数の画像（以下、ピクチャと呼ぶ）からなる動画像信号を圧縮符号化し、この圧縮符号化した動画像信号を、記録媒体の一例としての光ディスクに記録する例を挙げている。
【0011】図1において、端子２００には上記複数のピクチャからなる動画像信号Ｓ３１が入力されている。ビデオエンコーダ２０２は、入力された現在のピクチャの画像信号を目標符号化ビット量になるようにエンコードする。上記ビデオエンコーダ２０２での圧縮符号化により得られた符号化ビットストリームＳ３２は、送信バッファ（以下、エンコーダバッファ２０３と呼ぶ）へ入力される。
【0012】このエンコーダバッファ２０３は、入力ピクチャ毎の発生符号量の変動を平滑化し、所定のビットレートでビットストリームを出力するためにある。このエンコーダバッファ２０３から読み出されたビットストリームＳ３３は、多重化器（マルチプレクサ）２０４へ入力される。
【0013】なお、図1では示していないが、この多重化器２０４へは、例えばオーディオ信号を圧縮符号化した符号化ビットストリーム等も入力されており、多重化器２０４は、それら複数の入力ビットストリームを時分割で多重化し、一つのビットストリームにする。
【0014】この多重化器２０４から出力されたビット

ストリームは、ＥＣＣエンコーダ２０５によってエラーコレクションコードが付加され、スイッチ２１０を介して主変調回路２０６に送られる。

【００１５】この主変調回路２０６では、スイッチ２１０を介して供給されたＥＣＣエンコーダ２０５の出力ビットストリームに対して、所定の変調処理、例えばいわゆるＤＶＤ（ディジタルビデオディスク、あるいはディジタルバーサタイルディスク）に使用されているＥＦＭ＋の変調等の処理を施す。この主変調回路２０６の出力データは記録ヘッド２０７に送られ、この記録ヘッド２０７にて信号Ｓ３４が光ディスク２０８に記録される。

【００１６】さらに本実施の形態のシステムでは、鍵発生回路２０１から暗号化データ（暗号化鍵、暗号化ルール）が発生され、この暗号化データに基づき、上記エンコーダバッファ２０３の読み出しアドレスを制御することにより、上記符号化ビットストリームＳ３２のスクランブルが行われる。すなわち、当該エンコーダバッファ２０３からは、上記符号化ビットストリームＳ３２が上記暗号化データに基づいてスクランブルされたビットストリームＳ３３が出力される。したがって、上記信号Ｓ３４として光ディスク２０８に記録された上記ビットストリームは、上記暗号化データに基づくスクランブルが行われたデータで構成されていることになる。

【００１７】また、鍵発生回路２０１の暗号化データ（暗号化ルール）の情報は、上記ビデオエンコーダ２０２からのビデオデータ（及びオーディオデータ）とともに、上記エンコーダバッファ２０３にデータとして供給される。さらにこのエンコーダバッファ２０３に供給された暗号化データは、上記多重化器２０４に送られ、ＥＣＣエンコーダ２０５によってエラーコレクションコードが付加された後、スイッチ２１０に送られる。当該暗号化データは、最終的には光ディスク２０８上の所定の領域（セクタ）に書き込まれることになる。

【００１８】ここで、この暗号化データについて、従来と同様にビットストリームとして所定のセクタに書き込むようにすると、すなわち、オーディオ及びビデオデコーダ（ＡＶデータ）のビットストリームの場合と同様に主変調回路２０６で変調を施して所定のセクタに書き込むようにすると、当該暗号化データは容易に復調及び解析されてしまい。そして、そのビットストリームも容易に解読できてしまうことになる。

【００１９】そこで、本実施の形態では、この暗号化データのビットストリームについては、スイッチ２１０を切り替えて副変調回路２０９に送り、当該副変調回路２０９によって上記主変調回路２０６とは全く異なるアルゴリズムを用いた変調方式にて変調を施すようにしている。すなわち、主変調回路２０６が８－１６変調のＥＦＭ＋の変調である場合、上記副変調回路２０９では例えばいわゆるＣＤ（コンパクトディスク）に使用されている８－１７変調であるＥＦＭ等の変調方式を使用する。

【００２０】このことにより、光ディスク２０８上には、同一サイズのセクタや誤り訂正ブロックの中に、異なる変調方式でコード変換されたコード列が存在することになる。また、ＡＶデータのビットストリームと暗号化データのビットストリームとでは、ワードの切れ目も相互に異なることになり、したがって、通常の再生装置にて暗号化データを再生しようとしたときにその再生装置を誤動作させる効果が得られることになる。

【００２１】なお、この副変調回路２０９の変調方式については、公開しないものとする。

【００２２】次に、本実施の形態システムにおける再生系（デコード系）の構成について、図２を用いて説明する。本実施の形態では、再生系についても、記録系の主変調回路２０６と副変調回路２０９にそれぞれ対応する少なくとも２つの復調回路が存在する。

【００２３】図２において、再生系では、再生ヘッド３０１により、光ディスク２０８からデータが読み出される。

【００２４】ここで、セクタアドレスに基づいて読み出しが開始されると、先ず最初に光ディスク２０８上の所定のセクタを読み出し、暗号化データのビットストリームを得る。この暗号化データのビットストリームは、副復調回路３０８により、例えば１－７ＲＬＬの復調がなされる。

【００２５】当該復調された暗号化データは、ＥＣＣデコーダ３０３により誤り訂正がなされ、その後この誤り訂正がなされたデータは、デマルチプレクサ３０４により各種データと他のデータとに分離される。

【００２６】デマルチプレクサ３０４にて分離された暗号化データは、バッファ３０５を介して鍵解除回路３０７に送られ、ここに登録される。当該鍵解除回路３０７に登録された暗号化データは、暗号化鍵として他のデータのデスクランブルに使用される。

【００２７】次に、通常のＡＶデータのセクタから読み出されたビットストリームは、主復調回路３０２により、例えばＥＦＭ＋の復調がなされる。

【００２８】当該復調されたＡＶデータのビットストリームは、ＥＣＣデコーダ３０３により誤り訂正がなされ、その後この誤り訂正がなされたデータは、デマルチプレクサ３０４により各種データと他のデータとに分離される。すなわち、このときのデマルチプレクサ３０４では、多重化されているビデオデータとオーディオデータを分離する。上記分離されたビデオデータはバッファ３０５に送られ、同じく分離されたオーディオデータは図示を省略したオーディオ信号処理系に送られる。

【００２９】上記バッファ３０５に送られたデータは、前記記録系において暗号化データに基づいたスクランブルがなされているデータであり、このバッファ３０５では、鍵解除回路３０７に登録された暗号化データに基づいて読み出しアドレスを制御することにより、当該スク

ランブルされているデータのデスクランブルが行われる。

【００３０】上記バッファ３０５からの上記デスクランブルされたデータ（圧縮されているビデオデータ）は、ビデオデコーダ３０６に送られ、当該ビデオデコーダ３０６にて圧縮が解かれ、ビデオ信号として出力される。

【００３１】ここで、本発明が不正な複製を防止できる理由について説明する。

【００３２】従来は、多重化ビットストリームに対する変調方式としては、一つの変調方式のみが規定されており、また、互換性を維持するため、その変調方式は完全に公開されている。例えば、前述のＤＶＤに採用されたＥＦＭ＋という変調テーブルは、８ビットの入力ワードに対する１６ビットの変調ワードが定義されている。この変調テーブルは１６ビットの取り得るワードから、「１」や「０」の連続する個数や累積ＤＣの値（ＤＳＶ）を考慮して、最適な組み合わせが選定されている。従って、この変調方式で互換を取る限り、光ディスク上のビットストリームは、暗号であっても何らかのコード（文字コード）として読むことが可能である。このため、当該コードを解析すれば、暗号の法則性を見つけだすことができ、その結果、不正なコピーが可能となってしまう。

【００３３】これに対して、本発明に示したように、あるセクタのみを別の変調方式（例えばＥＦＭ）で変調してあると、そのビットストリームを主変調回路２０６の変調方式によるコードワードとして、ＥＦＭ＋の復調回路（主復調回路３０２）で復調をした場合、ＥＦＭ＋では定義していないワードが含まれている可能性があり、正常な復調ができなくなる。また、ＥＦＭ＋とＥＦＭとでは、コードワード長が１６ビットと１７ビットとで異なることから、コードワードの分離さえできない。

【００３４】従って、あたかも当該セクタにエラーがあるかのように、後段のＥＣＣデコーダ３０３は検知し、ＥＣＣによるエラー訂正を行おうとする。しかし、ＥＣＣについても訂正するための正常なパリテイが無いため、バーストエラーとして、誤動作をしてしまう。従って、当該セクタに書かれている文字列（すなわち暗号化データ）そのものを検出することができない。

【００３５】なお、副変調回路２０９における変調方式（副変調方式）としては、１セクタ程度の短い時間であるため、ＤＳＶが問題とならず、どのような変調方式でも使用することができる。また、数多く存在する変調方式において、同じ変調方式であっても対応コードワードの規則性を変更することにより、あたかも別物の変調方式のごとくコードワードが発生することになる。従って、全ての変調方式やそのコードワードの入れ替えを試すことは難しく、通常の技術を有するものであっても、副変調方式を特定することは困難である。

【００３６】また、本発明実施の形態にかかる主変調回路及び副変調回路と主復調回路及び副復調回路を、他の周辺回路と一体（１チップ化）し、副変調回路及び副復調回路だけを独立して動作させることができないようにすることで、いわゆるリバース・エンジニアリングを防止することも可能となる。

【００３７】

【発明の効果】本発明のデータ処理方法においては、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成し、特定のセクタには他のセクタのデータを正常にデコードするためのデータを書き込むことにより、また、本発明のデータ記録再生装置においては、それらの変調信号を記録媒体に記録する手段と、特定のセクタのデータを少なくとも二つの復調方式のうちの一により復調する手段と、特定のセクタの復調されたデータに基づき、他のセクタの復調データの正常再生を可能にする手段とを有することにより、暗号化鍵の管理が容易で且つ演算量も少なく、簡単なシステムでも実現でき、したがって、安価で簡単な構成であっても不法コピーを有効に防止し得る暗号化が可能となる。

【００３８】すなわち本発明によれば、少なくとも二つの変調方式により、特定のセクタについて他のセクタとは異なる変調方式でコードワードを生成することとしたため、何れの変調方式も特定されない限り、特定のセクタのコードワードの復調をすることができない。従って、この特定のセクタに書き込まれた再生許可の鍵情報が復調できない限り、他のセクタの正常な再生もできないようにすることができる。

【図面の簡単な説明】

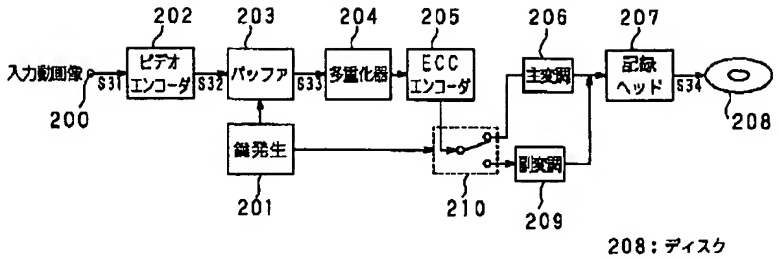
【図１】本発明実施の形態のシステムの記録系（エンコード系）の概略構成を示すブロック回路図である。

【図２】本発明実施の形態のシステムの再生系（デコード系）概略構成を示すブロック回路図である。

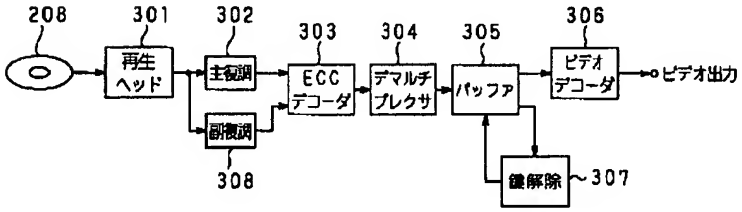
【符号の説明】

２０２　ビデオエンコーダ、　２０３　エンコーダバッファ、　２０４　多重化器、　２０６　主変調回路、　２０７　記録ヘッド、　２０８　光ディスク、２０１　鍵発生回路、　２０９　副変調回路、　２１０　スイッチ、　３０１再生ヘッド、　３０２　主復調回路、　３０３　ＥＣＣデコーダ、　３０４デマルチプレクサ、　３０５　バッファ、　３０６　ビデオデコーダ、　３０７鍵解除回路、　３０８　副復調回路

【図1】


202
203
204
205
206
207
入力動画像
S31
ビデオエンコーダ
S32
バッファ
S33
多重化器
ECCエンコーダ
主変調
記録ヘッド
S34
200
208
鍵発生
副変調
201
210
209
208：ディスク

【図2】


208
301
302
303
304
305
306
再生ヘッド
主復調
ECCデコーダ
デマルチプレクサ
バッファ
ビデオデコーダ
ビデオ出力
副復調
308
鍵解除
307